SalesHero Security Overview

With extensive experience in the financial services, telecommunication and government industries, we understand the complex security needs of a data platform to fulfill internal and regulatory requirements.

Authentication & Authorization

SalesHero provides multiple options for authenticating and managing end users including, LDAP, Active Directory (AD) OAuth2 and SAML. Administrators can configure SalesHero to use their existing LDAP, Active Directory system or OAuth2 framework and SAML as the system of record for centralized management. This includes user identity and credentials.

End users can authenticate into SalesHero using familiar credentials, which are checked against LDAP/AD/OAuth2/SAML on every login and they are identified as a member of group(s) just like in LDAP/AD including rested groups and multiple domains. Access to SalesHero is denied if the remote system no longer sanctions the end user to simplify SalesHero administration and allow users to use common credentials for SalesHero access. All authentication history is captured and stored in dedicated logs to facilitate security audits.

SalesHero provides role-based access with delegation, reserving certain actions for administrators only. Artifacts remain under the control of the author until shared at the group level. This applies to data stores, sources, uploaded files, data flows, and sinks.

SalesHero supports connectivity to LDAPS (often called LDAP over SSL). LDAP communications between applications are not encrypted by default.

Custom roles allow IT to control which users can perform specific tasks within the SalesHero application. The viewing, creation and execution of flows (such as ingest and analytics) are governed by role membership, as are performance of administrative functions and the scope of artifact sharing.

SalesHero maintains a “private folder” of data in distributed file systems or network attached storage. Access to raw and imported data and analyses results can be restricted by a user.

Encryption

AI data is encrypted during transport and storage (at rest). Encryption strength and algorithms are customizable.

To secure traffic between the end-user's browser and the SalesHero application server, SalesHero supports the use of HTTPS (HTTP over SSL). This requires a simple configuration change to SalesHero and for end-users to use the correct URL.

All end user credentials, data store passwords and keys (SSH, EC2, etc.) maintained by SalesHero are masked in the UI and encrypted in the SalesHero metadata store.

Security

As some implementations need to be optimized for security and some for performance, SalesHero allows granular configurations of individual security capabilities, including:

- Pluggable encryption algorithms and strength
- Encryption of data from source to data flow
- Encryption of data from data flow to sink
- Encryption of any temporary written data (e.g. when data needs to be cached for a reduce-side join)
- Encryption key rotation (on request)
- Encryption of all communication between the node if configured
- Https access for the web-based admin console
- Integration into authentication providers such as OAuth, OAuth2, LDAP, SAML or Microsoft Active Directory
- Audit and access logs

General Data Protection Regulation (GDPR) Compliance

SaleHero is GDPR-complaint based on the below measures and is configurable based on the customer's policy.

- Any company using SalesHero and their respective customers have the right to access, or the right to obtain confirmation as to what purpose SalesHero is processing their data
- Any company using SalesHero and their respective customers can easily update their own personal information to keep it accurate
- Any company using SalesHero and their respective customers have the right to request SaleHero erase their data, cease its dissemination and have third parties discontinue processing their data
- SalesHero maintains confidentiality through data encryption
- SalesHero automatically deletes unused data (configurable)
- SaleHero excludes opt-out customer data points (configurable)
- Data use is based on purpose limitation and data minimization